

Information Technology Laboratory Newsletter

INSIDE THIS ISSUE

ITL Focuses on Automated Image-Based Tattoo Recognition

ITL Promotes the Adoption of Elliptic Curve Cryptography

ITL's Work in Biometrics Makes an Impact in Mexico

ITL Hosts Major Conference on Mathematical Functions

Staff Accomplishments

Selected New Publications

Upcoming Technical Conferences



Credit: Katherine Green, NIST

July—August 2015

Issue 136

ITL Focuses on Automated Image-Based Tattoo Recognition

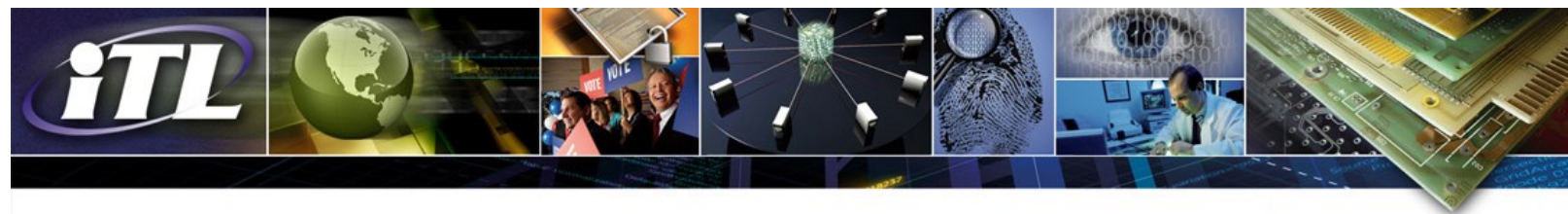
ITL researchers are working to develop automated methods to recognize tattoos in images, a technology which would provide significant advantages to law enforcement agencies nationwide. To advance this effort, ITL recently hosted the Tattoo Recognition Technology – Challenge (Tatt-C) Workshop, where an international group of experts from industry, academia, and government gathered at NIST to discuss challenges and potential approaches to automated image-based tattoo recognition. The goals of the workshop were to discuss current law enforcement use cases and state-of-the-art algorithm performance against those use cases, examine technical successes and challenges, share utility and perspectives on the operational use of tattoos, identify gaps and needs to support and progress future development, and identify potential follow-on development and evaluation activities.

The six research teams that participated in the Tatt-C program presented their methodologies, current algorithm performance, and recommendations on progressing development. The participating organizations included MorphoTrak (U.S.), Purdue University (U.S.), the MITRE Corporation (U.S.), Compass Technical Consulting (U.S.), the Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (Germany), and the Alternative Energies and Atomic Energy Commission (France).

Additionally, a panel of U.S. government agencies with operational needs for image-based tattoo recognition technology, including the Federal Bureau of Investigation (FBI) Scars, Marks, Tattoos Services Team, the FBI Cryptanalysis and Racketeering Records Unit, the Department of Homeland Security Homeland Security Investigations, the National Center for Missing and Exploited Children, the Michigan State Police, and the NIST lead for the American National Standards Institute Biometric Data format standard shared their perspectives on current shortcomings of the existing keyword-based tattoo collection and retrieval process and the drivers for an image-based capability.

Computer vision methods applied to representing and matching tattoo images were discussed. Sessions on best practices for tattoo collection and annotation, and defining tattoo similarity identified a number of activities that might advance the technology.

The highlights from the Tatt-C workshop were recently published in [Nature Magazine](#). More information about Tatt-C and the proceedings of the workshop are available on the [Tatt-C website](#).



ITL Promotes the Adoption of Elliptic Curve Cryptography

More than 15 years have passed since NIST first standardized elliptic curve cryptography for digital signature algorithms. The current state of the art has advanced. In research and other standards venues, newer curves have been proposed which pursue better performance or simpler and more secure implementations. To respond to this advance of technology, ITL recently sponsored the [Workshop on Elliptic Curve Cryptography \(ECC\)](#).

Presentations included proposals for new elliptic curves, an overview of the use of ECC in industry, new applications, and requirements and the process for standardizing new elliptic curves. The workshop provided a venue to engage the crypto community, including academia, industry, and government users, to discuss possible approaches to promote the adoption of secure, interoperable, and efficient elliptic curve mechanisms.

ITL's Work in Biometrics Makes an Impact in Mexico

The Asamblea Legislativa del Distrito Federal (ALDF) (Legislative Assembly of the Federal District) for Mexico City has installed a system for electronic voting using members' fingerprints. The ALDF is the law-making body for the over 21 million people of Mexico City's Federal District. The new voting system is based on a biometric device command and control protocol, developed in ITL, called Web Services-Biometric Devices (WS-BD). The protocol allows a tablet computer (where the voting application runs) to control the biometric scanners that are mounted within members' individual physical desk-top computers. WS-BD provided the system developers with an efficient and effective way to add biometric capabilities to devices that would otherwise have no built-in support for biometrics. More information on the [NIST Biometric Web Services](#) project is available.

ITL Hosts Major Conference on Mathematical Functions

Some 200 attendees from 34 countries participated in the recent 13th International Symposium on Orthogonal Polynomials, Special Functions, and Applications (OPFSA). Only the second instance of this biennial conference to be held in North America, the meeting was cosponsored by the ITL Applied and Computational Mathematics Division and the Society for Industrial and Applied Mathematics. Conferences in this series provide a forum for mathematicians, physicists, computational scientists, and

application scientists in other fields to communicate recent research results on mathematical functions, which play an essential role in analytical and computational investigations in all areas in science and engineering. The OPSFA community provides the technical basis for the [NIST Digital Library of Mathematical Functions \(DLMF\)](#), an online source of reference information on this topic.

Staff Accomplishments

Ram Sriram received a 2015 Distinguished Career in Engineering Sciences Award from the Washington Academy of Sciences. The award recognized contributions and technical leadership in developing computational tools and techniques for engineering design and for enabling interoperability of CAD/CAM/CAE systems.

Randall Easter received a Technical Excellence Award from the InterNational Committee for Information Technology Standards (INCITS). The award recognized his numerous contribution to the INCITS/CS1 – Cyber Security standards community during a tenure of more than ten years.

ITL recognized the following contributions of selected staff members during 2014-2015:

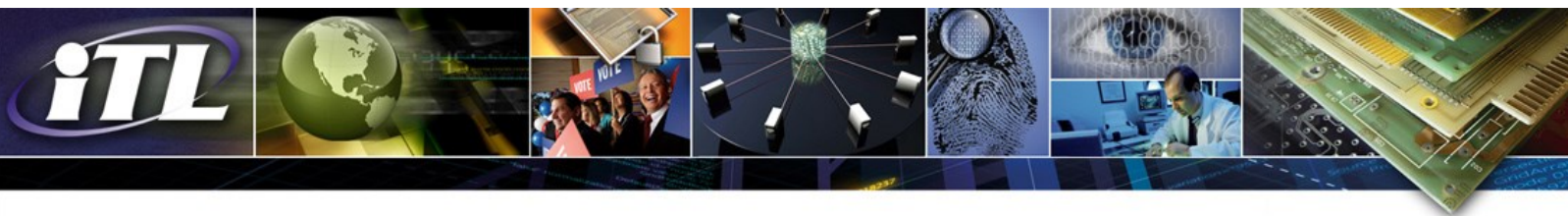
ITL Outstanding Contribution: **Scott Glancy**, for technical and analytical excellence in the advancement of quantum tomography and its application to quantum optics experiments with light and microwaves.

ITL Outstanding Conference Paper: **Yi-Kai Liu**, for excellence in research and exposition in the paper "Single-Shot Security for One-time Memories in the Isolated Qubits Model."

ITL Outstanding Journal Paper: **James Sims**, for excellence in research and exposition in the paper "Hylleraas-Configuration-Interaction Nonrelativistic Energies for the 1 S Ground States of the Beryllium Isoelectronic Sequence."

ITL Outstanding Administrative Support: **Janet Madison**, for extraordinary service and dedication and her willingness to undertake any support task beneficial to ITL.

ITL Associates of the Year: **Harold Affo, Diane Azais, Frederic DeVaulx, Nicolas Crouzier, Antoine Gerardin, Julien Perugini, Caroline Rosin, Salifou Sidi, Sheryl Taylor, and Jungyub Woo**, for developing the 2014 and 2015 R2 Editions of the Health IT Test Method, which is used to certify Electronic Health Record systems.



Selected New Publications

[Interfaces for Personal Identity Verification](#)

By David Cooper, Hildegard Ferraiolo, Ketan Mehta, Salvatore Francomacaro,

Ramaswamy Chandramouli, and Jason Mohler
NIST Special Publication 800-73-4, Parts 1-3
May 2015

FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, defines procedures for the PIV life-cycle activities including identity proofing, registration, PIV Card issuance, and PIV Card usage. FIPS 201 also specifies that the identity credentials must be stored on a smart card. SP 800-73-4 contains the technical specifications to interface with the smart card to retrieve and use the identity credentials. The specifications reflect the design goals of interoperability and PIV Card functions. The goals are addressed by specifying a PIV data model, card edge interface, and application programming interface. Moreover, SP 800-73-4 enumerates requirements where the standards include options and branches.

[Guide to Industrial Control Systems \(ICS\) Security](#)

By Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn
NIST Special Publication 800-82, Revision 2
May 2015

This document provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations, while addressing their unique performance, reliability, and safety requirements. The document provides an overview of ICS and typical system topologies, identifies typical threats to these systems, and provides recommended security countermeasures.

[Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations](#)

By Ron Ross, Patrick Viscuso, Gary Guissanie, Kelley Dempsey, and Mark Riddle
NIST Special Publication 800-171
June 2015

The protection of Controlled Unclassified Information (CUI) while residing in nonfederal information systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions and business operations. This publication provides federal agencies with recommended requirements for protecting the confidentiality of CUI.

[It's About the Face Impostor Distribution](#)

By P. Jonathon Phillips, Amy N. Yates, Geof H. Givens, and J. Ross Beveridge
NISTIR 8051
April 2015

This report presents a study of the effects of factors on the false accept rate (FAR) for three modern video face recognition algorithms. We examined the effects of environment (location), video (imagery)-based, and demographic factors. The study is performed on the handheld video in the Point and Shoot Face Recognition Challenge (PaSC), which consists of 1401 handheld videos of 265 subjects. The results of our analysis are consistent across the three algorithms. Our analysis shows that FAR can significantly vary.

[Face Recognition Vendor Test \(FRVT\) – Performance of Automated Gender Classification Algorithms](#)

By Mei Ngan and Patrick Grother
NISTIR 8052
April 2015

NIST performed a large-scale empirical evaluation of facial gender classification algorithms, with participation from five commercial providers and one university, using large operational datasets comprised of facial images from visas and law enforcement mugshots, leveraging a combined corpus of close to one million images. Using a lights-out, black-box testing methodology, core gender classification accuracy was baselined over a large dataset composed of images collected under well-controlled pose, illumination, and facial expression conditions, then assessed demographically by gender, age group, and ethnicity. Analysis on commonly benchmarked “in the wild” (i.e., unconstrained) datasets was conducted and compared with those from the constrained dataset. Assessments of classification performance on sketches and gender verification accuracy were documented.

[Applied and Computational Mathematics Division, Summary of Activities for Fiscal Year 2014](#)

Ronald F. Boisvert, Editor
NISTIR 8056
April 2015

This report summarizes recent technical work of ITL's Applied and Computational Sciences Division. Part I provides a high-level overview of the Division's activities, including highlights of technical accomplishments during the previous year. Part II provides further details on eight projects of particular note this year. Part III gives brief synopses of all technical projects active during the past year. Part IV lists publications, technical talks, and other professional activities in which Division staff members participated.



Upcoming Technical Conferences

8th Cloud Computing Forum and Workshop

Dates: July 7-10, 2015

Place: NIST, Gaithersburg, Maryland

Sponsor: NIST

Cost: None

This event will show federal leadership and support for the NIST technology role in U.S. Government agency adoption of cloud computing to reduce costs and improve services and to strengthen relationships with the private sector. The first day will focus on cloud standards (organized by ISO/IEC JTC1 SC38) followed by three days of talks and panels centered on specific areas of research and development in the cloud environment. The event will cover the current state of cloud computing standards; progress on NIST Special Publication 500 293: 10 high-level requirements for cloud adoption; cloud forensics; and cloud computing: customers and government.

NIST contact: Robert Bohn, robert.bohn@nist.gov

Lightweight Cryptography Workshop 2015

Dates: July 20-21, 2015

Place: NIST, Gaithersburg, Maryland

Sponsor: NIST

Cost: \$55 (includes coffee breaks/refreshments)

\$20 (no coffee breaks/refreshments)

When current algorithms can be engineered to fit into the limited resources of constrained environments, their

performance is typically not acceptable. NIST seeks to discuss issues related to the security and resource requirements of applications in constrained environments, and potential future standardization of lightweight primitives.

NIST contact: Kerry McKay, kerry.mckay@nist.gov

BioImage Informatics Conference 2015

Dates: October 14-16, 2015

Place: NIST, Gaithersburg, Maryland

Sponsor: NIST

Cost: \$304 (with catering)

\$165 (without catering service)

\$100 – full-time students

This conference will bring together researchers and practitioners in the field of image informatics for the life sciences. The conference will cover a wide range of topics including applications to cell therapy, digital pathology, and regenerative medicine; data mining and machine learning of image information; advanced visualization of bioimages and image-derived information; storage and repositories of biological datasets; collaborative frameworks, pipelines, and environments; fundamental algorithms; advanced imaging approaches and instruments; reproducibility and large-scale imaging experiments; and other topics relevant to life science imaging and image informatics.

NIST contact: Peter Bajcsy, peter.bajcsy@nist.gov

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.



The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST). As a world-class measurement and testing laboratory encompassing a wide range of areas of computer science, mathematics, statistics, and systems engineering, our research program supports NIST's mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. ITL cybersecurity experts collaborate to develop cybersecurity standards, guidelines, and associated methods and techniques for federal agencies and industry. Our mathematicians and statisticians collaborate with measurement scientists across NIST to help ensure that NIST maintains and delivers the world's leading measurement capability. ITL computer scientists and other research staff provide technical expertise and development that underpins national priorities such as cloud computing, the Smart Grid, homeland security, information technology for improved healthcare, and electronic voting. We invite you to learn more about how ITL is enabling the future of the nation's measurement and standards infrastructure for information technology by visiting our website at <http://www.itl.nist.gov>.

ITL Editor: Elizabeth B. Lennon
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900
Phone: (301) 975-2832
Fax: (301) 975-2378
Email: elizabeth.lennon@nist.gov

Credit: Katherine Green, NIST

TO SUBSCRIBE TO THE
ELECTRONIC EDITION OF THE
ITL NEWSLETTER, GO TO
[ITL HOMEPAGE](#)